(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number : **0 597 599 A2**

(12) EUROPEAN PATENT APPLICATION

(21) Application number : **93308337.0**

(51) Int. Cl.[5] : **G06F 1/00**

(22) Date of filing : **20.10.93**

(30) Priority : **30.10.92 US 968693**

(43) Date of publication of application :
18.05.94 Bulletin 94/20

(84) Designated Contracting States :
DE FR GB IT SE

(71) Applicant : **AMERICAN TELEPHONE AND TELEGRAPH COMPANY**
32 Avenue of the Americas
New York, NY 10013-2412 (US)

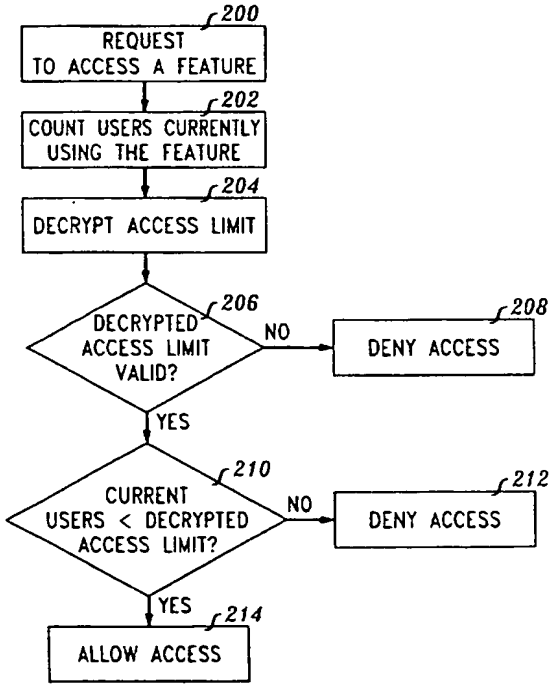
(72) Inventor : **Lassers, Harold Aaron**
265 Illinois Street
Elmhurst, Illinois 60126 (US)

(74) Representative : **Watts, Christopher Malcolm Kelway, Dr. et al**
AT & T (UK) Ltd. 5, Mornington Road
Woodford Green Essex, IG8 0TU (GB)

(54) Method for establishing licensor changeable limits on software usage.

(57) A system and method for establishing licensor changeable limits on shared software usage without the licensor having access to the system on which the shared software is running. An encrypted numerical limit value is embedded in the licensed software (program); when the program is executed ("accessed"), as a first step, the program decrypts the limit value (204) and compares it to the number of users currently accessing the shared program (210). If the number of users is less than the limit, then access is allowed (214). If the number of users is equal to (or greater than) the limit, then access is denied (212).

FIG. 2



EP 0 597 599 A2

Technical Field

This invention relates to the field of data processing, and, more specifically, to the field of limiting access to software wherein the limit may be changed by the licensor.

Background of the Invention

In software licensing agreements, especially for multi-user software, licensors commonly include contractual limits on the number of users who may have access to the software, the number of simultaneous users, and/or the number of total accesses. This is particularly important in licenses for multi-user software packages used in telephone switching systems where software-controlled features are licensed on a per-line basis. A problem in the art is that there is no effective method of enforcing and policing such agreements even with audits of software usage and/or site inspections.

Summary of the Invention

This problem is solved and a technical advance is achieved in the art by a method for establishing licensor changeable limits on shared software usage without the licensor having access to the system on which the shared software is running. An encrypted numerical limit value is embedded in the licensed software (program); when the program is executed ("accessed"), as a first step, the program decrypts the limit value and compares it to the number of users currently accessing the shared program. If the number of users is less than the limit, then access is allowed. If the number of users is equal to (or greater than) the limit, then access is denied. The licensor may supply the licensee with a new encrypted limit value to raise the number of allowed accesses.

Since the licensee does not have access to the encryption algorithm, it cannot change the limit value. If the licensee attempts to enter a random string as the encrypted limit value and the decrypted value is not valid, then access is denied to everyone. Furthermore, the number of accesses to the encrypted value may be limited (i.e., two or three times a week), to prevent the licensee from attempting to determine the encryption algorithm.

In the context of a telephone switching system, features provided to customers are generally controlled by shared software packages ("programs"). In this context, each time a customer is allowed access to a protected feature, the encrypted limit is decrypted and compared with the number of users currently using the feature. If the number of users is less than the limit, then the user is allowed to use the feature. Otherwise, the user is not allowed to use the feature. The encrypted limit, an alphanumeric string, can be changed using standard field update facilities.

Brief Description of the Drawing

FIG. 1 is a block diagram of a switching network configuration, including an exemplary embodiment of this invention;

FIG. 2 is a flow chart of the general implementation of an exemplary embodiment of this invention;

FIG. 3 is an exemplary maintenance screen as displayed on the maintenance console of FIG. 1 illustrating an update of the encrypted alphanumeric string;

FIG. 4 is an exemplary maintenance screen as displayed on the maintenance console of FIG. 1 illustrating an update of user access to a shared feature; and

FIG. 5 is a flow chart describing another exemplary embodiment of this invention.

Detailed Description

This invention will be described in connection with the telephone switching system, as illustrated in FIG. 1, but the application of this system is much broader. For example, a method for establishing license or changeable limits on shared programs according to this invention may be used in a general purpose, program-controlled computer system.

The telephone switching network configuration of FIG. 1 has two central office switches, 100 and 200, and inter-switch signaling network 250, e.g., a common channel signaling (CCS7) network and illustrative communications stations, including conventional analog telephone station sets 23, 25, and 201, an integrated services digital network (ISDN) telephone set 11, and data terminal 13. Switches 100 and 200 are interconnected by communication path 26, which may include intermediate switches.

Illustratively, switch 100 is a distributed control ISDN electronic switching system such as the system disclosed in U.S. Patent 4,592,048, issued to M. W. Beckner, et al., on May 27, 1986. Alternatively, switch 100 may be a distributed control, analog or digital switch, such as a 5ESS® switch manufactured by AT&T and described in the AT&T Technical Journal, v. 64, No. 6, July/August, 1985, pages 1303-1564.

Switch 100 includes a number of switching modules (SMs 110, 120, 130), each associated with a different set of telephone station sets or trunks. Each switching module includes a control unit for controlling connections to and from its associated telephone station sets or trunks. Switching module 110, for example, includes control unit 110 for controlling connections to and from telephone station set 11. Switching module 120 includes control unit 121 for controlling connections to and from station set 23. Each control

unit comprises a processor 125 and memory 126. Each memory 126 includes a database 127, wherein processor 125 stores configuration and operational data, as is known in the art. For example, lists of features associated with telephone station sets 23 and 25 are stored in database 127. Features such as call forwarding, three-way calling, and the like are controlled by software programs stored in memory 126, and executed by processor 125, using data stored in database 127.

The architecture of switch 100 includes communication module (CM) 150 as a hub with switching modules 110, 120, and 130, and an administrative module (AM) 160 emanating therefrom. AM 160 provides maintenance and provisioning information and commands to SMs 110, 120, and 130, as is known in the art, from maintenance terminal 165.

Switching module 110 terminates digital subscriber lines, e.g. 12. Switching module 120 terminates conventional analog lines (i.e., tip ring pairs), 22, 24, and provides circuit-switched c/nnections to and from associated telephone sets 23, and 25. Switching module 130 is similar to switching modules 110 and 120, but includes the appropriate analog or digital trunk unit (not shown) for interfacing with the outgoing trunks included in communication path 26 to switch 200. To complete the description of switch 100, communication module 150 acts as a switch fabric for communication among switch modules and administrative module (AM) 160. Switch 200 is shown connected to a conventional analog telephone station set 201, for purposes of illustration. The architecture of switch 200 and the types of telephone station sets served by switch are not important to the present invention and are thus not described further.

In the context of switch 100, the method for establishing licensor changeable limits on software usage can be used illustratively to limit the number of telephone subscribers who can subscribe to a particular feature, for example, call forwarding. It is well known in the art that features such as call forwarding are licensed by switch vendors to customers (operating companies) on a per-line basis. For example, call forwarding may be provided on switch 100 for 5,000 lines. It is in the licensor's interest, therefore, to have a mechanism that limits the number of lines (users) that may use call forwarding at any given time. If the operating company has more users that want call forwarding than the limit allows, the operating company may request and pay for additional line allocations, wherein the vendor may supply a new limit.

Turning now to FIG. 2, a flow chart for a general case of this invention is shown. During the building of the executable program that controls the switching system, a library is linked into the program, as is known in the art, controlling the feature program (in this example the call forwarding feature), which includes a decryption algorithm and a routine to determine whether to allow access to the program. This routine follows the general flow chart shown in FIG. 2. Starting in box 200, a request is received to access a particular feature. In box 202 a count is made of the users currently using the feature. In box 204 the access limit is decrypted using the algorithm loaded when the program was built. The specific encryption algorithm is not important to this invention, as any encryption algorithm may be used without departing from the scope of this invention. It is to the licensor's benefit, of course, to have a difficult encryption algorithm to prevent licensees from reverse engineering the encryption algorithm.

Processing continues to decision diamond 206 where a determination is made whether the decrypted access limit is valid. The decrypted limit is compared to a range of known values. If the limit is out of range or does not decrypt into a numerical value, then it is presumed that the encrypted access limit has been tampered with. Therefore, if, in decision diamond 206, the decryption access limit is not valid, then access to the feature is denied in box 208.

If, in decision diamond 206, the decrypted access limit is valid, then processing proceeds to decision diamond 210, where a determination is made if the number of users is less than the decrypted access limit. If the number of users is greater than the decrypted access limit, then, in box 212, access to the feature is denied. If the number of current users is less than the decrypted access limit, then in box 214, access is allowed.

Turning now to FIG. 3, a screen as displayed on maintenance terminal 165 (FIG. 1) is shown, illustrating the access limit update screen. As stated above, the encrypted access limit may be changed. This feature is advantageous when, for example, the licensee desires to have more users access a particular feature, for example, call forwarding. The licensee would pay for the increased number of lines to use the feature, and the licensor would provide the licensee with a new encrypted access limit. In FIG. 3, a string representing an encrypted access limit is shown at 300. The string may be changed using the maintenance console keyboard. Field 310 shows the current access limit, which is the maximum allowable users for the particular feature. Field 310 equals the decrypted access limit 300. 320 shows the number of users currently accessing the protected feature. Preferably, the encrypted access limit field 300 may be changed only a few times over a predetermined time period. For example, allowing changes to the encrypted access limit field 300 three times a week, aids in preventing a licensee from attempting to reverse engineer the encryption algorithm by replacing the field randomly until a valid string is found.

Turning now to FIG. 4, a screen showing a feature selection list for a particular subscriber (user) is shown. When the licensee allows a subscriber access

to a feature, for example, call forwarding, the licensee updat%s the subscriber's profile. A typical update screen is shown in the example of FIG. 4. The subscriber is identified by telephone number and then a list of available features is displayed. For example, call forwarding 400 is allowed for this subscriber. Call waiting 410 and three-way calling 420 are not allowed. When call forwarding 400 is allowed, that is, the "NO" is changed to "YES", as illustrated. During such updates, the licensed software checks to determine if the licensee has reached the license limit for allowing access to the shared software (i.e., the call forwarding feature). If the license limit has been reached, the software will not allow the update. In this example, the "YES" will automatically turn to "NO".

This embodiment is further useful when ISDN subscribers may turn features on or off by themselves at any given time. A screen (such as FIG. 4), may be displayed at a remote terminal 13 (FIG. 1), controlling features for telephone 11 (FIG.1). Up to 5,000 subscribers may use call forwarding at any given time, but the operating company may allow more than that number of subscribers the ability to use call forwarding. In this example, when a subscriber attempts to turn on a feature, the licensed software may permit only 5,000 subscribers to use call forwarding.

This invention may also be used to limit the absolute number of telephone subscribers (users) subscribing to features such as call forwarding. A maintenance screen such as FIG. 4 is displayed each time a telephone subscriber feature is changed. When a change is made (changing a "NO" to "YES" in field 400 to allow this subscriber to use call forwarding, for example), the system checks to determine whether the limit of the number of subscribers that have call forwarding available has been reached. If the subscriber limit has not been reached, then the feature is allowed for this subscriber. If the limit is reached, then the feature is denied.

A further use for this invention is to turn software (program) protected by this invention "OFF" as provided by the licensor, and then "ON" after a license fee is paid. The encrypted alphanumeric string sets a limit of zero for turning the program "OFF" and sets a limit of infinity for "ON". This may be useful, for example, when software is provided with a system as an option that may be turned on later. The licensor does not have to supply different or additional software for each customer. The licensor merely supplies the appropriate encrypted string according to what the licensee has paid for.

This invention may also be used to control the total number of accesses which may be made to a feature. In other words, this invention may be used to allow a licensee to use a particular feature 5,000 times and no more. This aspect of this invention may be useful, for example, for software operable on a personal computer, or other system where the licensee may desire a limited license to use software. In this embodiment, each time any user attempts to access the license feature, a check is made of the total number of previous accesses, which is compared with the license limit. Both the access limit and the count of the total number of previous accesses are stored in encrypted form to prevent unauthorized change. FIG. 5 illustrates a flow chart according to this embodiment of the invention.

In box 500, a request is made to access the program, and, in box 502, the count of previous accesses is decrypted from an encrypted, stored value. Processing continues to decision diamond 504 where a determination is made if the decrypted count is valid. The decrypted count may not be valid if it is out of a certain range or alternatively does not decrypt into a numeric value. The count may be out of range or non-numeric if the licensee attempts to change the encrypted count of previous accesses. If the decrypted count is not valid, then access is denied in box 506. If in decision diamond 504 the decrypted count is valid, then processing continues to box 508 where the access limit is decrypted. Processing continues to decision diamond 510 where a determination is made if the decrypted access limit is valid. The parameters for validity of the limit are generally the same as for the decrypted count. If the decrypted access limit is not valid, then access is denied in box 512.

If the decrypted access limit is valid in decision diamond 510, then processing continues to decision diamond 514 where the determination is made if the count is less than the limit. If the count is not less than the limit, then access is denied in box 516. If the count is less than the limit, then in decision diamond 514 processing continues to box 518 where the count is incremented. In box 520, the count is then encrypted so that it may be stored in a form that the licensee cannot modify. Processing ends in box 522 where access is allowed to the feature or software.

Claims

1. A method for providing licensor control of the number of users accessing one or more licensed programs in a computer system arranged to execute a plurality of licensed programs, wherein one or more of said plurality of licensed programs is accessible by a plurality of users, without said licensor having access to said computer system, said method comprising the steps of:

   requesting access to said program (200);

   establishing a limit value by decrypting a portion of a previously encrypted alphanumeric string provided by said licensor (204);

   comparing said limit value to the number of users currently accessing said program (210);

denying access to said program if said number is greater than said limit value (212); and

allowing access to said program if said number is less than said limit value (214).

2. A method according to claim 1 wherein said encrypted alphanumeric string may be updated by said licensee replacing said encrypted alphanumeric string with a further encrypted alphanumeric string provided by said licensor, thus permitting said licensor to change the limit value of the number of users.

3. A method according to claim 2 wherein the number of licensee updates of said encrypted alphanumeric string over a predetermined period of time is limited to aid in preventing said licensee from determining the encryption algorithm.

4. A method according to claim 1 further comprising the step of verifying that said limit value is a valid numeric value after said step of decrypting said encrypted alphanumeric string; and

denying access to said licensed program if said limit value is not a valid numeric value, so that said licensee cannot replace said encrypted alphanumeric string with random values in order to circumvent the encryption algorithm.

5. A method of limiting the number of accesses to a licensed program in a computer system arranged to execute said licensed program, wherein said licensed program is accessible a limited number of times, said limit being set by a licensor, without said licensor having access to said computer system comprising the steps of:

requesting access to said program (500);

establishing a number of accesses by decrypting a previously encrypted first alphanumeric string (502);

establishing a limit by decrypting a previously encrypted second alphanumeric string (508);

comparing said limit to the number of accesses (514);

if said number of accesses is equal to or greater than said limit, denying access to said feature (516); and

if said number of accesses is less than said limit, allowing access to said feature (522), incrementing said number of accesses (518), and encrypting said number of accesses into said first alphanumeric string (520).

6. A method according to claim 5 wherein said second encrypted alphanumeric string may be updated by a licensee replacing said second encrypted alphanumeric string with a further encrypted alphanumeric string provided by said licensor, thus permitting a licensor to change the limit value of the number of accesses without having access to said computer system.

7. A method according to claim 6 wherein the number of updates of said second encrypted alphanumeric string over a predetermined period of time is limited to prevent a licensee from determining the encryption algorithm.

8. A method according to claim 5 further comprising the steps of verifying that said number of accesses is a valid numeric value after said step of decrypting said first encrypted alphanumeric string;

verifying that said limit is a valid numeric value after said step of decrypting said second encrypted alphanumeric string; and

denying access to said licensed program if said number of accesses or said limit is not a valid numeric value, to prevent said licensor from replacing said first or second encrypted alphanumeric string with random values in order to circumvent the encryption.

9. A method for providing licensor control to limit the number of users accessing one or more features simultaneously in a telephone switching system providing a plurality of features, wherein one or more of said features is accessible by a plurality of users, without said licensor having access to said switching system, said method comprising the steps of:

requesting access to said feature;

establishing a limit value by decrypting a portion of a previously encrypted alphanumeric string provided by said licensor;

comparing said limit to the number of users currently accessing said feature;

denying access to said feature if said number is greater than said limit; and

allowing access to said feature if said number is less than said limit.

10. A method according to claim 9 wherein said encrypted alphanumeric string may be updated by a licensee replacing said encrypted alphanumeric string with a further encrypted alphanumeric string provided by said licensor, thus permitting a licensor to change the limit value of the number of users without having access to said system.

11. A method according to claim 10 wherein the number of updates of said encrypted alphanumeric string over a predetermined period of time is limited to aid in preventing a licensee from circumventing the encryption algorithm.

FIG. 2

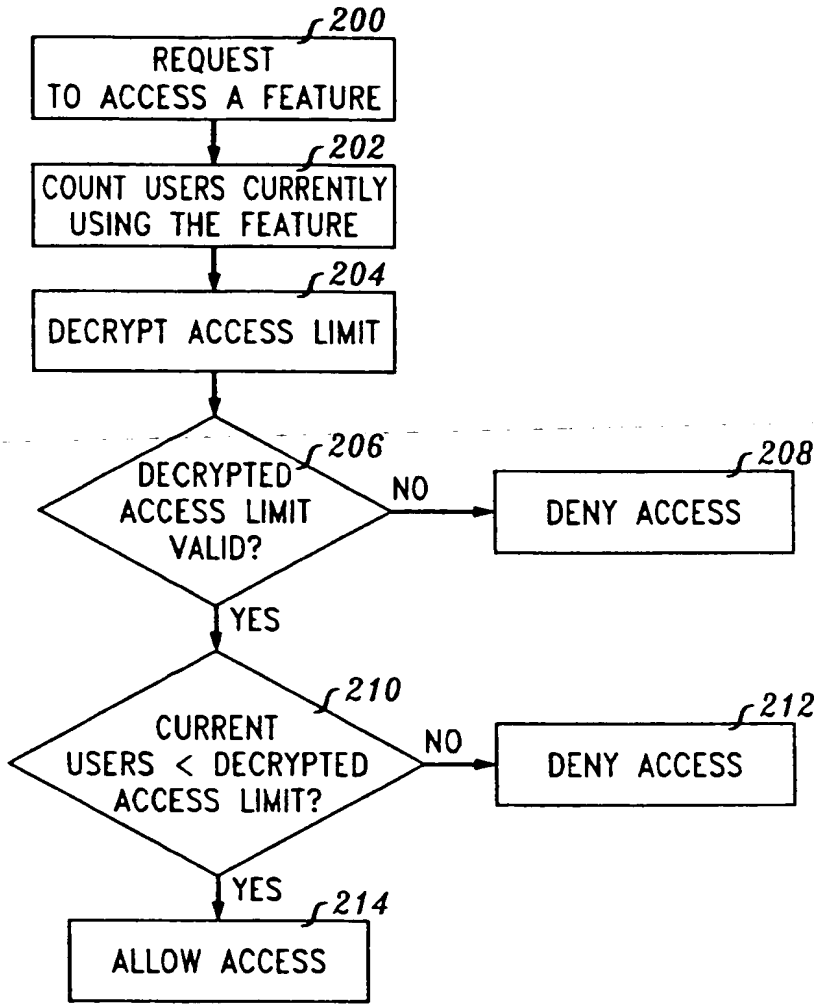

200
REQUEST TO ACCESS A FEATURE
202
COUNT USERS CURRENTLY USING THE FEATURE
204
DECRYPT ACCESS LIMIT
206
DECRYPTED ACCESS LIMIT VALID?
NO
208
DENY ACCESS
YES
210
CURRENT USERS < DECRYPTED ACCESS LIMIT?
NO
212
DENY ACCESS
YES
214
ALLOW ACCESS

FIG. 3

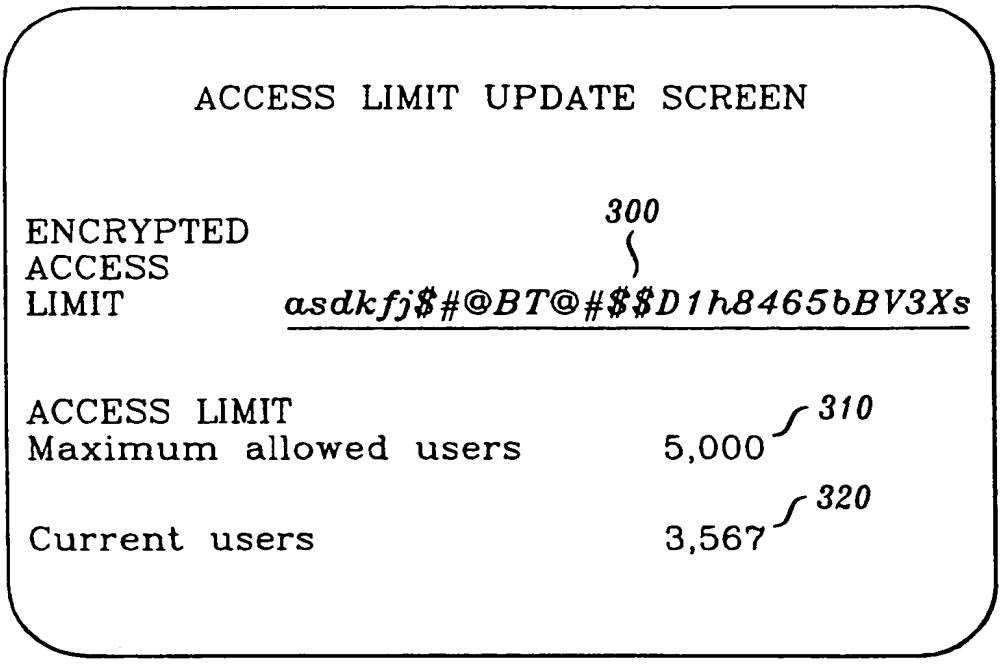

ACCESS LIMIT UPDATE SCREEN
300
ENCRYPTED ACCESS LIMIT
asdkfj$#@BT@#$$D1h8465bBV3Xs
ACCESS LIMIT
Maximum allowed users
5,000
310
Current users
3,567
320

FIG. 4

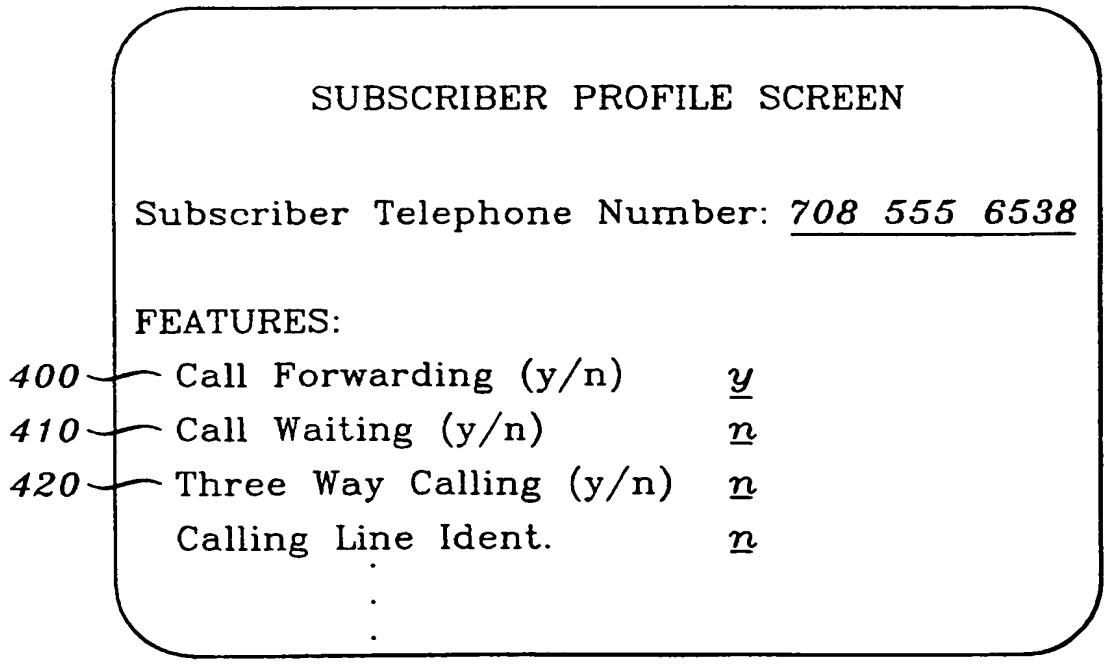
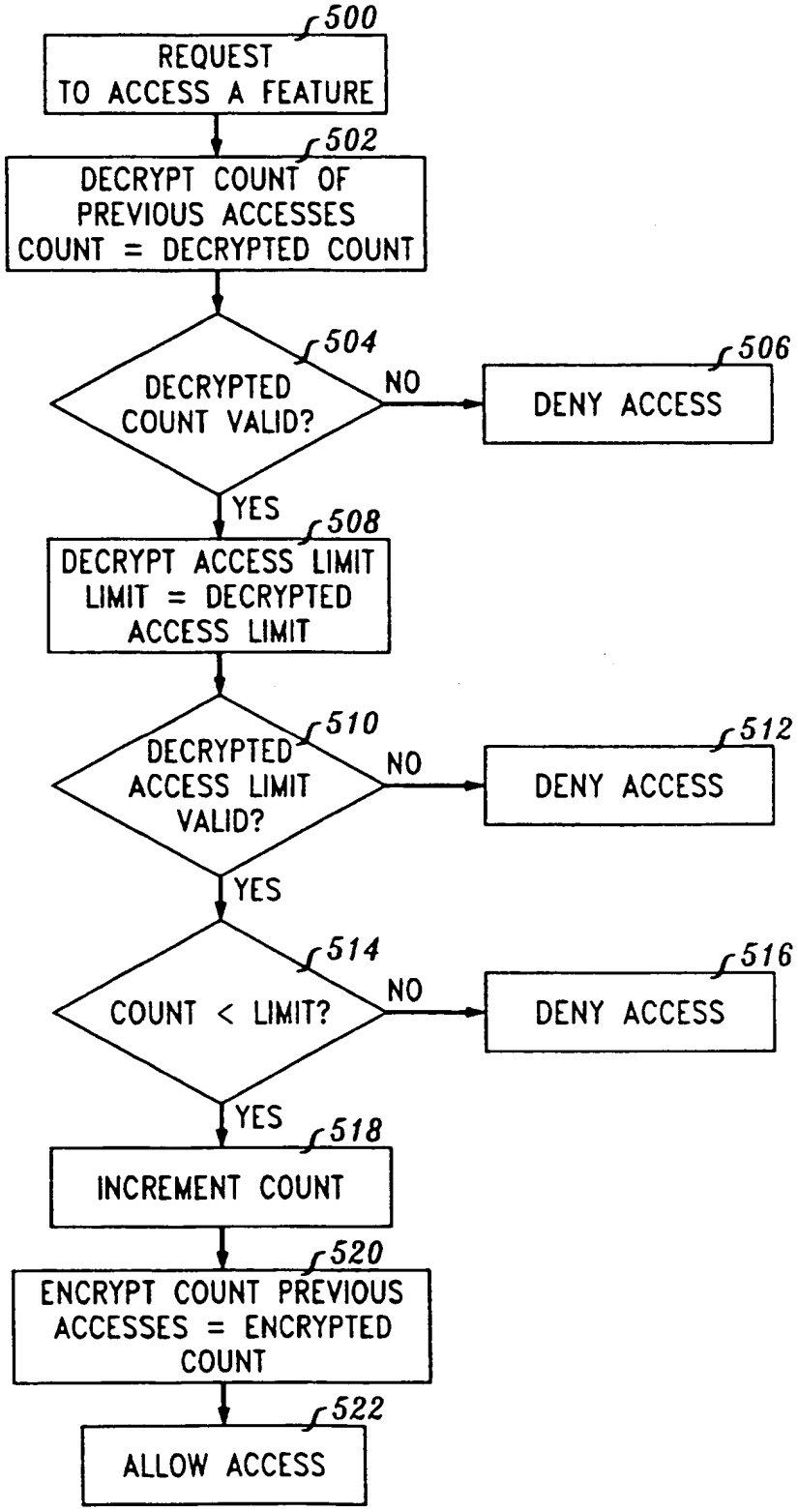

SUBSCRIBER PROFILE SCREEN
Subscriber Telephone Number: 708 555 6538
FEATURES:
400
Call Forwarding (y/n) y
410
Call Waiting (y/n) n
420
Three Way Calling (y/n) n
Calling Line Ident. n

FIG. 5


500
REQUEST TO ACCESS A FEATURE
502
DECRYPT COUNT OF PREVIOUS ACCESSES COUNT = DECRYPTED COUNT
504
DECRYPTED COUNT VALID?
NO
506
DENY ACCESS
YES
508
DECRYPT ACCESS LIMIT LIMIT = DECRYPTED ACCESS LIMIT
510
DECRYPTED ACCESS LIMIT VALID?
NO
512
DENY ACCESS
YES
514
COUNT < LIMIT?
NO
516
DENY ACCESS
YES
518
INCREMENT COUNT
520
ENCRYPT COUNT PREVIOUS ACCESSES = ENCRYPTED COUNT
522
ALLOW ACCESS

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number : **0 597 599 A3**

(12) EUROPEAN PATENT APPLICATION

(21) Application number : **93308337.0**

(51) Int. Cl.[5] : **G06F 1/00**

(22) Date of filing : **20.10.93**

(30) Priority : **30.10.92 US 968693**

(43) Date of publication of application :
18.05.94 Bulletin 94/20

(84) Designated Contracting States :
DE FR GB IT SE

(88) Date of deferred publication of search report :
10.08.94 Bulletin 94/32

(71) Applicant : **AT & T Corp.**
32 Avenue of the Americas
New York, NY 10013-2412 (US)

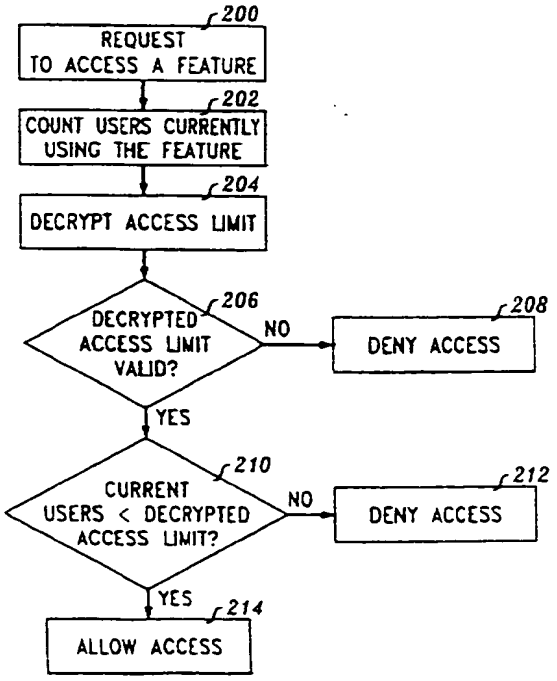
(72) Inventor : **Lassers, Harold Aaron**
265 Illinois Street
Elmhurst, Illinois 60126 (US)

(74) Representative : **Watts, Christopher Malcolm Kelway, Dr. et al**
AT&T (UK) Ltd.
5, Mornington Road
Woodford Green Essex, IG8 0TU (GB)

(54) Method for establishing licensor changeable limits on software usage.

(57) A system and method for establishing licensor changeable limits on shared software usage without the licensor having access to the system on which the shared software is running. An encrypted numerical limit value is embedded in the licensed software (program) ; when the program is executed ("accessed"), as a first step, the program decrypts the limit value (204) and compares it to the number of users currently accessing the shared program (210). If the number of users is less than the limit, then access is allowed (214). If the number of users is equal to (or greater than) the limit, then access is denied (212).

FIG. 2



EP 0 597 599 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 93 30 8337

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.5)
Y	US-A-5 023 907 (JOHNSON ET AL) * abstract; figure 2 * * column 2, line 3 - column 5, line 29 * ---	1-16	G06F1/00 H04Q3/00
Y	TRANSACTIONS OF THE INSTITUTE OF ELECTRONICS AND COMMUNICATION ENGINEERS OF JAPAN, vol. E73, no. 7 , July 1990 , TOKYO, JP; pages 1133 - 1146 R.MORI ET AL 'Superdistribution: The Concept and the Architecture' * the whole document * ---	1-16	
Y	1988 INTERNATIONAL ZURICH SEMINAR ON DIGITAL COMMUNICATIONS, 10 March 1988 , ZURICH, CH; pages 45 - 52 K.SIUDA 'Security Services in Telecommunications Networks' * the whole document * ---	9-16	
A	EP-A-0 384 610 (IBM) * abstract * * page 1, line 1 - page 3, line 36 * ---	1-16	TECHNICAL FIELDS SEARCHED (Int.Cl.5) G06F H04Q
A	EP-A-0 367 700 (IBM) * abstract; figure 2 * * column 7, line 5 - line 45 * ---	2,3,6,7, 10,11, 14,15	
	-/--		

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	17 June 1994	Powell, D

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 93 30 8337

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.5)
A	IEEE TRANSACTIONS ON COMMUNICATIONS, vol. COM-29, no. 4 , April 1981 pages 376 - 385 D.G.HAENSCHKE 'Network Management and Congestion in the U.S. Telecommunications Network' * page 379, left column, line 9 - page 380, left column, line 3 * * page 381, right column, line 47 - page 383, right column, line 15 *	9-16	

TECHNICAL FIELDS SEARCHED (Int.Cl.5)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	17 June 1994	Powell, D

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number : **0 597 599 A3**

(12) EUROPEAN PATENT APPLICATION

(21) Application number : **93308337.0**

(51) Int. Cl.[5] : **G06F 1/00**

(22) Date of filing : **20.10.93**

(30) Priority : **30.10.92 US 968693**

(43) Date of publication of application :
18.05.94 Bulletin 94/20

(84) Designated Contracting States :
DE FR GB IT SE

(88) Date of deferred publication of search report :
10.08.94 Bulletin 94/32

(71) Applicant : **AT & T Corp.**
32 Avenue of the Americas
New York, NY 10013-2412 (US)

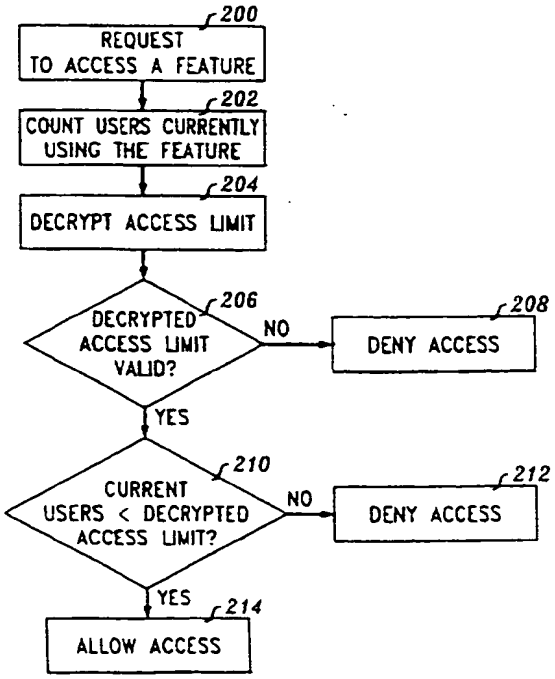
(72) Inventor : **Lassers, Harold Aaron**
265 Illinois Street
Elmhurst, Illinois 60126 (US)

(74) Representative : **Watts, Christopher Malcolm Kelway, Dr. et al**
AT&T (UK) Ltd.
5, Mornington Road
Woodford Green Essex, IG8 0TU (GB)

(54) Method for establishing licensor changeable limits on software usage.

(57) A system and method for establishing licensor changeable limits on shared software usage without the licensor having access to the system on which the shared software is running. An encrypted numerical limit value is embedded in the licensed software (program); when the program is executed ("accessed"), as a first step, the program decrypts the limit value (204) and compares it to the number of users currently accessing the shared program (210). If the number of users is less than the limit, then access is allowed (214). If the number of users is equal to (or greater than) the limit, then access is denied (212).

FIG. 2



BEST AVAILABLE COPY

EP 0 597 599 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 93 30 8337

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.5)
Y	US-A-5 023 907 (JOHNSON ET AL) * abstract; figure 2 * * column 2, line 3 - column 5, line 29 * ---	1-16	G06F1/00 H04Q3/00
Y	TRANSACTIONS OF THE INSTITUTE OF ELECTRONICS AND COMMUNICATION ENGINEERS OF JAPAN, vol. E73, no. 7 , July 1990 , TOKYO, JP; pages 1133 - 1146 R.MORI ET AL 'Superdistribution: The Concept and the Architecture' * the whole document * ---	1-16	
Y	1988 INTERNATIONAL ZURICH SEMINAR ON DIGITAL COMMUNICATIONS, 10 March 1988 , ZURICH, CH; pages 45 - 52 K.SIUDA 'Security Services in Telecommunications Networks' * the whole document * ---	9-16	
A	EP-A-0 384 610 (IBM) * abstract * * page 1, line 1 - page 3, line 36 * ---	1-16	TECHNICAL FIELDS SEARCHED (Int.Cl.5) G06F H04Q
A	EP-A-0 367 700 (IBM) * abstract; figure 2 * * column 7, line 5 - line 45 * ---	2,3,6,7, 10,11, 14,15	
	-/--		

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	17 June 1994	Powell, D

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 93 30 8337

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.5)
A	IEEE TRANSACTIONS ON COMMUNICATIONS, vol. COM-29, no. 4 , April 1981 pages 376 - 385 D.G.HAENSCHKE 'Network Management and Congestion in the U.S. Telecommunications Network' * page 379, left column, line 9 - page 380, left column, line 3 * * page 381, right column, line 47 - page 383, right column, line 15 *	9-16	

TECHNICAL FIELDS SEARCHED (Int.Cl.5)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	17 June 1994	Powell, D

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)